Designation: D8217 – 20

Standard Guide for Access Control System[1]

This standard is issued under the fixed designation D8217; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers the recommended access control system for protecting resin cannabis, resin cannabis products, resin cannabis waste, currency, people, property, and assets.

1.2 *Units*—The values stated in inch-pound units are to be regarded as standard. The values given in parentheses are mathematical conversions to SI units that are provided for information only and are not considered standard.

1.3 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use. The recommendations herein are offered as the minimum requirement. All standards are subject to the requirements of the local Authority Having Jurisdiction (AHJ) in any given area.*

1.4 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Terminology

2.1 *Definitions of Terms Specific to This Standard:*

2.1.1 *access control software, n*—track staff by recording access point ingress activities while at the same time enhancing the overall safety of the property; sounds an alert when anomalies detected; accessibility via the Internet.

2.1.2 *authentication, v*—verifying the identity of a user for an access control device that ensures the individual using the device is authorized access.

2.1.3 *authority having jurisdiction (AHJ), n*—the organization, office, or individual responsible for issuing permits, approving layout drawings, equipment, enforcing the requirements of a code or standard or approving materials, an installation or procedure. Usually the AHJ is the building or fire official of the city or county in which the job site is located. In some cases, such as healthcare facilities, transient accommodations and day care facilities, the AHJ is the city or county building or fire official.

2.1.4 *digital video recorder (DVR), n*—records data in a digital format to a local or networked mass storage device.

2.1.5 *dual-locked storage container, n*—lock that require two individuals to open; the dual custody classified lock programmed to require two combinations or keys to open.

2.1.6 *electric strike, n*—operates by means of electric current, connected to an access control system, remotely monitored and controlled, both to lock and unlock.

2.1.7 *interlock, n*—whereby only a single door shall open at any point in time; once a door is open, all other doors in the room that are part of the interlock are prevented from opening.

2.1.8 *Internet protocol (IP), n*—data sent over the Internet or other network.

2.1.9 *magnetic lock, n*—large electro-magnet mounted on the door frame and a corresponding armature mounted on the door; when the magnet is powered and the door is closed, the armature is held fast to the magnet to secure the door.

2.1.10 *man trap, n*—locked room whereby only a single door shall open at any point in time; once a door is open, all other doors in the room that are part of the man trap are prevented from opening.

2.1.11 *personal identification number (PIN), n*—four- to six-digit code assigned to individuals and inputted onto a keypad for access.

2.1.12 *sally port, n*—locked enclosure for vehicles whereby only a single door shall open at any point in time; once a door is open, all other doors in the enclosure that are part of the sally port are prevented from opening.

2.1.13 *three-factor authentication, n*—at least three of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof.

2.1.14 *two-factor authentication, n*—at least two of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof.

[1] This guide is under the jurisdiction of ASTM Committee D37 on Cannabis and is the direct responsibility of Subcommittee D37.05 on Security and Transportation.

Current edition approved Feb. 1, 2020. Published February 2020. DOI: 10.1520/D8217-20.

2.1.15 *uninterruptible power supply (UPS), n*—ensure continuous operation of systems upon loss of normal power using a surge protector with a built-in backup battery.

3. Significance and Use

3.1 Access control system devices are installed at strategic locations, such as all exterior entrances, administrative offices, grow rooms, processing rooms, manufacturing rooms, storage areas, transaction areas, loading dock, vaults, and locker room.

3.2 Access control system software tracks staff by recording access point ingress and egress activities while at the same time enhances the overall safety of the property.

3.3 An access control system is especially important during an emergency to determine who is on and off the property.

3.4 Individuals are permitted access after they have been subjected to background screening and issued credentials that allow for real-time monitoring and forensic analysis of employee or vendor on-site movement.

3.5 All doors should also be secured with electric strike or magnetic locks that remain locked in the event of power loss (default secured).

3.6 Limited access area door locks, unlocks, and opens through the use of a two-factor authentication consisting of at least two of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof with a keyed override system installed.

3.7 Exterior door locks should be unlocked and opened through the use of a two-factor authentication consisting of at least two of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof with a keyed override system installed.

3.8 Restricted access area, such as a vault and safe are protected by three-factor authentication consisting of at least three of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof.

3.9 Growing, processing, manufacturing, transaction, product, and currency rooms should be protected by a minimum of two-factor authentication: at least two of the following: an access control credential (for example, badge, FOB, wireless device), personal identification number (PIN), or biometric, or combinations thereof.

3.10 Product or currency, or both should be stored in a dual-locked storage container with a lock that requires two individuals to open. The dual custody classified lock programmed to require two combinations or keys to open.

4. Summary of Guide

4.1 The following access control system technologies, equipment, capabilities, and procedures are industry best-practice-based.

4.1.1 An on- or off-site monitoring station is designed to manage access control information, along with receiving and sending alarm notifications.

4.1.2 Using access control technology, select personnel with designated backups are able to monitor and appropriately assign room access.

4.1.3 Access control cards are a standard-size credential visibly displayed with the name of the employee, contractor, or visitor on one side and a control number on the other, and full-time employee cards also contain a photo.

4.1.4 Individuals must possess their company-issued access control credentials at all times while on the property.

4.1.5 The access control credentials are programmed for specific days, hours, and rooms of access.

4.1.6 When an employee is terminated, the access control credential is collected and deactivated.

4.2 All requests for access control credentials are made through the system and allows authorized personnel to:

4.2.1 Request a credential for a new employee or contractor,

4.2.2 Request a replacement credential, and

4.2.3 Add additional access privileges to a current credential.

4.3 The ACS allows two or more doors in a room to be configured as an interlock, whereby only a single door shall open at any point in time. Once a door is open, all other doors in the room that are part of the interlock are prevented from opening.

4.3.1 Examples of an interlock area include man traps, controlled labs, and sally ports.

4.4 For highly secured areas, an extra level of authentication such as biometric readers can be required for access.

5. Policies and Procedures

5.1 Policies and procedures specifying instructional requirements applicable to the ACS to protect resin cannabis and currency, such as roles and responsibilities for responding to an alarm or an alert and notification protocols for alarms and alerts.

5.2 A complete index and guide to the hardware, software, devices, technical documentation, monitors and controls should be available either in hardcopy or electronic form.

5.3 This guide should include a map of the ACS locations, direction of coverage, position numbers and operating instructions for the ACS equipment. It is important that the door naming convention is documented in alignment with the location description. These descriptors should also be aligned with the floor plans so that service and maintenance is seamless. This is also critical for first responders should the need arise.

6. Maintenance Requirements

6.1 Access control system should be maintained in good working order at all times, per the manufacturer's specifications.

6.2 Conduct and document monthly maintenance inspections to ensure that any repairs, alterations or upgrades are made for proper operation of the system.